Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 07 April 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports a tractor−trailer loaded with an industrial chemical collided with a car and burned through the night, killing two people, closing a major highway, and causing evacuations in southeastern Kentucky. (See item 3)
- The San Francisco Chronicle reports colleges across the country, through computer security failure and human error, have exposed confidential information about hundreds of thousands of students and employees over the Internet. (See item 6)
- The Associated Press reports Texas police don't yet know who is responsible for at least 29 sticks of dynamite found strewn along roadsides near San Juan. (See item 22)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 06, New York Times* — **Utility could have halted '03 blackout, panel says. An Ohio power company should have prevented last summer's blackout across a wide swath of North America by intentionally cutting off electricity to most of the Cleveland area, American and Canadian officials said yesterday, April 5.** In their final report on the August 14 blackout that darkened much of the Midwest, the Northeast and Ontario, a panel convened by the two national governments put much of the blame on the FirstEnergy Corporation, one of

the nation's largest utilities, in whose eastern Ohio territory the collapse began. The inquiry found that FirstEnergy did not shut off some customers as a preventive measure and apparently did not have a plan for doing so on short notice. But Chuck Jones, senior vice president for energy delivery at FirstEnergy. said the international investigation had glossed over the problems created by a rise in long−distance power transmission in recent years. He said power being shipped from southern Ohio to Ontario, across FirstEnergy's territory, was one cause of the company's problems the day of the blackout.
Source: http://www.nytimes.com/2004/04/06/national/06BLAC.html

2. *April 06, The Free Lance−Star (Fredericksburg, VA)* — **Chemical leaks at North Anna.** A sheared pipe leaked about 500 gallons of a water−treatment chemical on the ground at North Anna Power Station over the weekend. The leak of the water−softening agent −− designed to keep water flowing through the nuclear power plant's turbines clean and free of algae and chemical deposits −− was reported to the Nuclear Regulatory Commission on Saturday. **"Most of it was absorbed into the ground," Richard Zuercher, a spokesman for Dominion Virginia Power's nuclear operations, said yesterday, April 5.** However, some of the chemical reached the plant's discharge canal, Zuercher said. The discharge canal is downhill from the treatment building and several hundred yards away. "We sampled the discharge canal and found no detectable amount in it," he said. No one was injured and no radioactivity was released, Zuercher said. **The breach, which was discovered at 1:14 p.m. on Saturday, April 3, was reported to the NRC a few minutes later. The North Anna plant sits on the Louisa County shoreline of the 13,000−acre Lake Anna.** The spill also was reported to the Virginia Department of Environmental Quality, which determined that it was contained on the plant site.
Source: http://www.freelancestar.com/News/FLS/2004/042004/04062004/1 321332

[Return to top]

Chemical Sector

3. *April 06, Associated Press* — **Two dead after chemical truck crashes. A tractor−trailer loaded with an industrial chemical collided with a car and burned through the night, killing two people, near London, KY. The crash also closed a major highway in southeastern Kentucky and led police to order evacuations in the rural area.** The two victims were in the truck, while the driver of the car was hospitalized in good condition, police said. The vehicles collided shortly before midnight about 10 miles north of London, state police said. London, KY, is about 80 miles south of Lexington. **The truck was carrying sodium hydrosulfite, which is poisonous if inhaled, said Stacy Floden of the state Division of Disaster and Emergency Services. The chemical is used in a variety of industrial processes.** The truck was hauling nine drums of the chemical in a crystalized form to Oshkosh, WI, Floden said. Two of the drums burst into flames and four plunged over the guard rail, she said. Interstate 75 and U.S. 25, which intersects the larger highway, were closed in both directions and remained shut down at late morning Tuesday, police said. An area within a one−mile radius of the truck was evacuated, including a gas station and a truck stop, Laurel County Deputy Sheriff Doug Thomas said. He said fewer than 25 people were involved in the evacuation.
Source: http://www.newsday.com/news/nationworld/nation/sns−ap−chemical−truck−crash,0,3506130.story?coll=ny−nationalnews−headline s

4. *April 06, Mobile Register (Mobile, AL)* — **Thirty homes evacuated. A tank spewing potentially dangerous hydrogen peroxide vapors prompted firefighters to evacuate about 30 homes on two streets and close a city park in south Mobile, AL, on Monday afternoon, April 5, fire officials said. The evacuation order remained in force overnight as the tank continued to vent, and it was not clear when the residents would be allowed to return home, said Steve Huffman, a spokesman for the Mobile Fire−Rescue Department.** Vapors were coming from the 1,500−gallon tank when a technician went to check on it at the end of Columbus Avenue off Navco Road near Dog River, according to Huffman. Firefighters were called to the scene at 2:10 p.m. A fire could ignite when vapors touch organic materials like leaves on surrounding trees, explained District Chief Douglas Cooper. Even though vapor dissipates rapidly in the air, firefighters were watching for that possibility Monday evening, Cooper said. A vapor cloud could have formed in the area if the tank ruptured, Huffman said. The vapor acts as an irritant to eyes and mucus membranes. **The tank, containing about 1,000 gallons of hydrogen peroxide solution, is owned by a Georgia company but leased by the Mobile Area Water and Sewer System for water purification, Huffman said.**
   Source: http://www.al.com/news/mobileregister/index.ssf?/base/news/1 08124304810270.xml

[Return to top]

Defense Industrial Base Sector

5. *April 06, Federal Computer Week* — **DoD expenditures. The Department of Defense (DoD) in 2003 spent $73 billion more on major programs than it did the previous year.** Defense officials this week released the department's annual selected acquisition reports (SARs) detailing the cost differences of major service programs. The report, submitted to Congress on December 31 of last year but not publicly released until April 6 of this year, lists a net annual increase of $73 billion, or 5.8 percent, for the costs of programs that have been in previous reports. The $73 billion overall increase in acquisition included higher program estimates, stretched development and procurement schedules, an increase of planned quantities to be purchased, application of higher escalation indices, higher support costs related to increased quantities, and additional engineering changes.
   Source: http://www.fcw.com/fcw/articles/2004/0405/web−sars−04−06−04. asp

[Return to top]

Banking and Finance Sector

6. *April 05, San Francisco Chronicle* — **Colleges leaking confidential data.** Colleges across the country, through computer security failure and human error, have exposed confidential information about hundreds of thousands of students and employees over the Internet, and experts say they expect the problems to continue. **In addition to being targeted by some very savvy hackers, college computer systems have been made vulnerable by the schools themselves through inadequately trained employees who have access to the files.** The problem has been highlighted in recent months by some high−profile breaches of computer−stored records including names, addresses, Social Security numbers and, in some

cases, even credit cards, for applicants, students, alumni and staff. Computer experts say that data erroneously posted on the Internet could have been copied or accessed before the problem was discovered, leaving individuals vulnerable for years. California State Senator Debra Bowen (D−Redondo Beach) authored legislation that requires government agencies, including the state's colleges and universities, to stop using Social Security numbers on student ID cards and public postings as of January.
Source: http://sfgate.com/cgi−bin/article.cgi?file=/c/a/2004/04/05/M NGGP60LNV1.DTL

7. *April 05, The Times (UK)* — **Secret hackers to aid war on internet fraud.** Fears that small online retailers are the weakest link in the fight against internet fraud have prompted MasterCard, the global payment scheme group, to set up secret teams of hackers to test security systems in the sector. The project, named Site Data Protection (SDP), will go live in May and will target online outlets that fail to comply with appropriate levels of internet security. **SDP teams will be recruited by the banks that have relationships with online merchants whose systems do not come up to scratch.** Organized criminal gangs are increasingly hacking into the systems of online retailers and stealing subscribers' credit card and personal details. The information can then be used to commit "card−not−present fraud"−−fraudulent buying of goods and services from a remote location, usually by phone or via the internet. **Card−not−present fraud is thought to be one of the world's fastest growing crimes.** Stolen personal details have also been used by gangs to commit "phishing", sending fake e−mails purporting to be from a bank or retailer to cardholders to trick them into revealing bank account details. MBNA and Barclays were recently victims of phishing.
Source: http://www.timesonline.co.uk/article/0,,5−1063208,00.html

8. *April 05, The Register* — **Scambusters target 419 online banks.** A new Website, "Artists against 419," has identified 53 fake banks and financial agencies, presumed to be Nigerian in origin. Most of these sites, with names such as Apextrustbank or Bondplc.com, are used in 419 advanced fee frauds. Some look truly plausible, until you notice their postal address. For instance, the Isle of Man is listed on one as being located on Dominica. Unfortunately, some do look strikingly real. **A couple are JavaScript−protected or use a 3rd party SSL service (security certificates) to give the impression they are legitimate.** Besides a few off−shore banks, most companies are registered in the Netherlands, South Africa and in the UK, and very often supported by web hosting companies from the U.S. Some hosting providers, however, do take action. **Since "Artists against 419" started operating, around 85 scam Websites have been removed.**
Source: http://www.theregister.co.uk/2004/04/05/scambusters_target_4 19_online_banks/

[Return to top]

Transportation Sector

9. *April 06, FOX News* — **Ridge: private sector must help fund security.** The federal government cannot afford to pay for the increased security needed to protect U.S. ports from terrorists, Department of Homeland Security Secretary Tom Ridge said Monday, April 5. Ports and shipping companies are facing a July 1 deadline to have security programs in place for their docks and vessels or face potential fines. The programs are based on regulations developed by the Homeland Security Department and the Coast Guard under the Maritime Transportation

Security Act of 2002. **The federal government plans to spend nearly $3 billion on security programs this year. Secretary Ridge noted the 360 ports protected by the Coast Guard do about $1 trillion in business every year. Sam Ruda, who heads the maritime division for the Port of Portland, said user fees likely will be needed to help pay the cost of increased security.**
Source: http://www.foxnews.com/story/0,2933,116253,00.html

10. *April 06, Associated Press* — **Florida airport getting tracking technology installed. Jacksonville International Airport will be one of the first in the country to track luggage with radio frequency identification tags, which officials believe will increase security and help reduce the number of lost bags.** The system is supposed to be installed by the fall, in time for February's Super Bowl in Jacksonville and the accompanying crush of travelers expected to use the airport, said Chip Snowden, chief operating officer of the Jacksonville Airport Authority. **By knowing exactly where luggage is along conveyor belts behind the airport's walls, the Transportation Security Administration believes any dangerous bags could be quickly located.** The small, paper−thin devices known as RFIDs work by using electronic readers to record data stored within microchips. The chips are encased in plastic tags laced with metal bands that serve as antennas, which transmit signals to monitoring devices. Tests have shown that the chips can be read with an accuracy rate of about 99%, better than the 85% typical with bar−code scanners.
Source: http://www.usatoday.com/tech/news/2004−04−05−jax−bags_x.htm

11. *April 06, Federal Computer Week* — **Coast Guard's modernization effort depends on new ships and new technology.** As the program executive officer for the Integrated Deepwater System, Rear Adm. Patrick Stillman oversees the multibillion−dollar, 20−year effort to revamp the fleet's physical assets while bringing the Coast Guard's technological force into the 21st century. **His vision centers on a Coast Guard that owes its success not only to newer ships and planes but also to a fully integrated information technology network that increases the timeliness, effectiveness and efficiency of all operations.** Similar to the Department of Defense's transformation and network−centric operations initiatives, Stillman said the service is working on a network−centric approach that is critical to the success of the Deepwater program. It demands the investment of so much time and money. "It's the network that really is the force multiplier here," Stillman said. "That's it in a nutshell, and that's where the investment is truly being made."
Source: http://www.fcw.com/fcw/articles/2004/0405/feat−deep−04−05−04 .asp

12. *April 05, Transportation Security Administration* — **TSA seeks private−sector proposals for registered traveler pilot program. Rear Adm. David M. Stone, Acting Administrator of the Transportation Security Administration (TSA), today, April 5, announced that the agency is seeking responses from the private sector to a Request for Proposal, also known as a Combined Solicitation Synopsis, for a Registered Traveler Pilot Program that will begin in select airports in late June.** Interested parties must describe in their response how they would provide program management, biometric capabilities, tactical operations and systems integration support. TSA plans to award the final contract in early June. "TSA continues to move forward with all possible speed to develop the Registered Traveler Program," Stone said. "Today's announcement is a major step in the process as TSA seeks to leverage knowledge and technology from private industry." To view the published Request for

Proposal, please visit the official Federal Business Opportunities Website at http://www.fedbizopps.gov.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 0097ca6

[Return to top]

Postal and Shipping Sector

13. *April 06, Atlanta Business Journal* — **UPS subsidiary to expand store network. United Parcel Service (UPS) Inc. subsidiary Mail Boxes Etc. has set a goal of expanding The UPS Store network to 5,000 locations in the U.S. by 2007, including stores in under−served areas such as urban neighborhoods, college campuses and military bases.** The move comes one year after 90 percent of Mail Boxes Etc. centers in the U.S. converted to The UPS Store name. UPS said that in its first year, The UPS Store network has generated triple−digit growth in UPS shipping volume and added more than 300 new stores.
Source: http://atlanta.bizjournals.com/atlanta/stories/2004/04/05/da ily19.html

[Return to top]

Agriculture Sector

14. *April 06, USAgNet* — **Canada announces kill of millions of birds in British Columbia. The British Columbia, Canada, poultry industry got its wish Monday, April 5, when the federal government said it approved its proposal to kill about 19 million chickens and turkeys throughout the Fraser Valley in a bid to wipe out contagious avian flu.** Agriculture Minister Bob Speller ordered the cull on the recommendation of the Canadian Food Inspection Agency (CFIA), "to stop the spread of this disease and to stamp it out." Affected poultry farmers had told Speller and his B.C. counterpart John van Dongen that it was the best way to get the industry back on track. **The affected area is sweeping, extending from Greater Vancouver to Hope, a two−hour drive east, north to the mountains and south to the U.S. border.** "This is going to be devastating for the poultry industry, not only farmers but others involved in the industry," said Rick Thiessen, president of the B.C. Chicken Growers Association. Many workers will have to be laid off and it could take six to eight weeks for all the birds to be destroyed.
Source: http://www.usagnet.com/story−national.cfm?Id=366&yr=2004

15. *April 06, Australian Associated Press* — **Cameras to detect crop disease.** Cameras mounted on airplanes may help farmers produce better crops and higher profits. **Scientists are testing the use of cheap digital cameras fitted with infra−red filters to identify crop diseases and other problems such as lack of water, long before they become obvious to growers on the ground.** Australian Department of Primary Industries extension officer Jim Barnes said although research was in its early days the system had already identified crop diseases and areas where there was not enough water being applied. "It's a cheap piece of technology, a digital camera mounted in a bubble on the door of the aircraft, but it could result in great cost savings for growers," Barnes said. If the system became a commercial reality a one−hour flight in a plane would cost around $300, but in that time 30 or more paddocks of crops could be

photographed. It was hoped the system would be proven successful by June next year after trials.
Source: http://www.theaustralian.news.com.au/common/story_page/0,5744,9206519%255E1702,00.html

16. *April 06, Agence France Presse* — **Avian flu feared in birds migrating to Russia. Several rooks that migrated recently to Russia's Far East from southeast Asia were found dead of suspected bird flu.** Environmentalists said they feared that the returning flocks might bring in the deadly bird flu after wintering in neighboring China, hard hit by an outbreak of the disease. Wild ducks spending the winter in China and coming back to the banks of the Amur river in Russia could be infected with the bird flu and contaminate Russian fowl, health officials said. **The whole of Russia's Far Eastern region is taking steps to protect poultry farms from possible contamination, they added.** Avian influenza has struck 10 Asian countries in recent months. Some 100 million chickens and other fowl have been culled in a massive regional effort to contain the spread of the highly pathogenic H5N1 flu strain.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20040406/hl_afp/russia_china_flu_040406100831

[Return to top]

Food Sector

17. *April 06, just−food.com* — **Smithfield completes sale of Schneider. U.S. meat processor Smithfield Foods has announced it has closed the sale of its wholly−owned Canadian subsidiary, Schneider Corporation, to Maple Leaf Foods for approximately $378 million.** The amount is subject to closing adjustments, including the assumption of the company's outstanding debt. Smithfield said it plans to use the net proceeds to repay the bridge loan used to finance its acquisition of Farmland Foods in October 2003.
Source: http://www.just−food.com/news_detail.asp?art=57201

18. *April 06, Reuters* — **Japan says no end to U.S. beef ban. Japan cannot end its ban on imports of U.S beef before May unless the United States "implements the same measures as we do" to prevent mad cow disease, the Japanese agriculture minister said in a letter made public on Tuesday, April 6.** Agriculture Minister Yoshiyuki Kamei's letter said the two nations needed to reach a consensus on how to assure beef is safe from the brain−wasting disease, but it did not repeat Japan's previous demand that all U.S. beef it imports be tested. U.S. meat industry officials noted the letter did not mention 100 percent testing of U.S. cattle, potentially an encouraging sign, but said there has been no overt change in position. Kamei said in the letter to U.S. Agriculture Secretary Ann Veneman that "careful discussions are necessary" to assess the U.S. risk of mad cow disease. Japan shut off imports of U.S. beef following the December 23 announcement of the first U.S. case of mad cow. **Japan was the number one market for U.S. beef exports until the mad cow case.**
Source: http://www.reuters.com/newsArticle.jhtml?type=businessNews&storyID=4764427&section=news

19. *April 05, Food Safety and Inspection Service* — **Bologna recalled. Charles T. Heard & Co., a**

Bangor, PA, firm, is voluntarily recalling approximately 100 pounds of ready−to−eat, fully cooked, bologna that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced April 5. The products were produced on March 31, 2004. They were distributed to two retail stores in Roseta and Wind Gap, PA, as well as the company's retail counter Bangor. FSIS has received no reports of illnesses associated with consumption of these products. The problem was discovered by the company. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/oa/recalls/prelease/pr011−2004.htm

[Return to top]

Water Sector

20. *April 07, KWTX (Texas)* — **Perchlorate study.** Perchlorate from an old Naval Weapons Industrial Reserve Plant site does not threaten the drinking water for half a million residents in central Texas, according to a federal study which could impact cities across the country. Local leaders met in McGregor Monday morning to deliver the good news. That perchlorate contamination that turned up in area waterways is not a risk to the half million Central Texans who drink the water. **Army Corps of Engineers Colonel John Minahan says, "Based on the data collected during this study, we found that water users are not at risk for exposure to perchlorate, consumption of cattle raised in the area presents no risk for exposure, and the bacteria in Lake Belton actually breaks down the perchlorate to harmless chemicals."** Congress commissioned the Army Corps of Engineers to study the effects of perchlorate three years ago.
Source: http://www.kwtx.com/home/headlines/664507.html

[Return to top]

Public Health Sector

21. *April 05, Associated Press* — **Researchers call for better infection control training.** Emergency workers need better training to keep infections from spreading, researchers from Saint Louis University told legislators Monday, April 5. **Paramedics often do not have proper training to handle emerging health threats, such as Severe Acute Respiratory Syndrome (SARS) or smallpox,** said Gene Carroll, the technical director for the Saint Louis University School of Public Health's Center for the Study of Bioterrorism and Emerging Infections. Carroll showed lawmakers a film in which paramedics responding to a hypothetical call would have transferred a disease from the infected person to their clothes, equipment, and all over the ambulance. His colleague, Bill Stanhope, told the Joint House and Senate Committee on Terrorism that training, not necessarily new supplies or gizmos, can help keep biological threats contained and protect workers, their families, and hospitals from contamination. **Carroll said that some of the most dangerous diseases now are spread by germs that can live for a long time outside the body, but safety procedures were established before such diseases were a concern.**
Source: http://www.kansascity.com/mld/kansascity/news/local/8361061. htm?1c

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *April 06, Associated Press* — **Texas police find dynamite along roadsides. Police said Monday, April 5, they have no idea who is responsible for at least 29 sticks of dynamite found strewn along roadsides near San Juan, TX.** Police Sgt. Rey Casarez said four sticks were found on a farm−to−market road on the south side of town Friday. He said 20 more were found Sunday strewn along the south side of town and around a residential area on the east side of town. Casarez said police had scoured the area, but hadn't found any more. "Still, that's a lot of sticks to be thrown around our city," he said. "We've walked the areas. We haven't been able to find more, but you never know." **McAllen's Emergency Response Team responded to the findings, along with officials with the federal bureau of Alcohol, Tobacco and Firearms.** Casarez said there were no markings on the dynamite. He said dynamite is a controlled substance and may have been left over from roadway or other construction projects.
Source: http://www.newsday.com/news/nationworld/nation/sns−ap−dynamite−found,0,4284497.story?coll=ny−nationalnews−headlines

23. *April 06, Associated Press* — **Maine gets anti−terrorism money. Radiation and chemical detection equipment and hazardous materials suits are among the equipment that Maine's fire and police departments plan to buy with more than $22 million in funding** announced Monday, April 5, by U.S. Sen. Susan Collins. Fire and police officials joined Collins, R−ME, as she presented a ceremonial check for $22.4 million. The funding is important because people turn to state and local agencies, not the federal government, when emergencies arise, she said. The heads of Portland's fire and police departments said that without such funding they could not afford to buy specialized anti−terror−related equipment. "This is equipment we need to fulfill our mission to protect our citizens," Portland Fire Chief Fred LaMontagne said. "This is equipment we could not purchase off our regular tax rolls."
Source: http://www.pressherald.com/news/state/040406terrorism.shtml

[Return to top]

Information and Telecommunications Sector

24. *April 02, CNET News.com* — **Wireless called key to global development. At a conference last week on using technology to solve social and economic problems in developing nations, a number of speakers emphasized the role of wireless communications.** A. Richard Newton, dean of the College of Engineering at the University of California, Berkeley, said the most important technological step to take in developing countries is to build out communications networks with wireless capabilities. He said **it is conceivable to put**

solar−powered antennae towers that support voice and data communications in villages for about $750 apiece. Newton also proposed a mobile phone with a much simpler interface, one he claimed was economically feasible. The phone would display images of people who called, so a user reviewing voice mail could press on the image of the person whose message he wanted to hear. Newton was among those participating in the "Bridging the Divide" conference organized by UC Berkeley's Management of Technology Program along with the United Nations Industrial Development Organization. The three−day event, held at the university's Haas School of Business, examined topics including health care technology, building environmentally sustainable industry, and technology essentials for economic development.
Source: http://news.com.com/2100−1001−5184405.html?tag=nefd_hed

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_NETSKY.P** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 1434 (ms−sql−m), 3127 (mydoom), 3128 (squid−http), 1080 (socks), 137 (netbios−ns), 2745 (urbisnet), 1025 (blackjack), 111 (sunrpc), 4899 (radmin) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

25. *April 06, Reuters* — **Terror attacks could rock stability. More attacks like the Madrid train bombs could destabilize global financial markets and pose a significant threat to their otherwise steady recovery, the International Monetary Fund (IMF) warned on Tuesday, April 6.** Economic activity has picked up and corporate balance sheets have strengthened since September, the IMF said in a optimistic Global Financial Stability Report. But attacks like those which killed about 190 people in Madrid on March 11 could throw a wrench in the works. "It is clear that if there were more incidents along the lines of Madrid, it would have an impact on the real economy, consumer confidence would be hit," said Gerd Haeusler, the IMF's Director of International Capital Markets. "I would be somewhat concerned that an additional risk premium would be built into some asset classes that would be quite unwelcome."
Source: http://money.cnn.com/2004/04/06/news/international/imf_repor t.reut/

26. *April 06, Reuters* — **Pakistan raids Islamic terror group. Pakistani police have arrested nine suspected Islamic militants in connection with a suicide bombing at a U.S. mission and a deadly attack on French nationals in 2002, a police official said on Tuesday, April 6.** The arrested men belonged to the shadowy Harkat−ul Mujahideen al−Alami and included the group's leader Syed Sohail Akhtar, alias Mustafa, said Police Chief Syed Kamal Shah. They were detained in city of Karachi in overnight raids, he said. Shah said the suspects were involved in a June 14, 2002, suicide bombing at the U.S. consulate in Karachi that killed 12 Pakistanis. The group also carried out a similar attack outside the Sheraton Hotel in Karachi in May 2002 that killed 11 French technicians.
Source: http://www.alertnet.org/thenews/newsdesk/ISL260073.htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP